**3GPP TSG-SA3 Meeting #115AdHoc-e draft\_S3-241113-r5**

**Electronic meeting, online, 15 - 19 April 2024** *revision of S3-24yyyy*

**Source: vivo, Interdigital, ZTE, Ericsson, OPPO, CATT, Qualcomm, Xiaomi, Lenovo, Apple, Nokia, Nokia Shanghai Bell**

**Title: Key issue on privacy for AIoT services**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve the pCR on new key issue on privacy for AIoT services.***

# 2 References

# 3 Rationale

This contribution proposes a new key issue on the privacy for AIoT services.

# 4 Detailed proposals

#### \*\*\* BEGIN CHANGES \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-49: "Study on Enhancement of support for Edge Computing in 5G Core network - Phase 3".

[xx] 3GPP TR 23.700-13: “Study on Architecture support of Ambient power-enabled Internet of Things”.

#### \*\*\* NEXT CHANGES \*\*\*

## 5.X Key issue #X: Privacy for AIoT services

### 5.X.1 Key issue details

5G Ambient IoT service is a type of cellular IoT communication system where Ambient IoT devices utilize harvested energy to generate RF signals for bi-directional information transmission. Ambient IoT devices are characterized by limited functions, requiring only small and infrequent data transfers and without the need for batteries.

TS 22.369 [x] clause 5.2.6 defines the following privacy-related requirements:

“The 5G system shall be able to provide a mechanism to protect the privacy of information (e.g., location and identity) exchanged during communication between an Ambient IoT device and the 5G network or an Ambient IoT capable UE.”

In AIoT services, identifier of AIoT device is exclusively used to identify the device and related information for the associated service. If the privacy of device ID is not ensured, an attacker can identify and track an AIoT device based on the device ID associated to the AIoT device. Thus, this key issue is to investigate potential mechanisms to ensure privacy of AIoT device identifiers.

### 5.X.2 Security Threats

If the privacy of device ID is not ensured, an attacker can identify and track an AIoT device based on the device ID associated to the AIoT device. If the device is used in a human wearable, then the location of the person wearing the wearable can be tracked.

Editor’s Note: security threat and requirement for potential exposure of quantity of devices after adversary broadcasts an inventory message is ffs.

### 5.X.3 Potential security requirements

The 3GPP System shall support for mitigating trackability and likability attacks on AIoT Devices.

NOTE: Not all AIOT services/device types are expected to require support of features to solve the above requirement and hence support of such features are not mandated.

#### \*\*\* END OF CHANGES \*\*\*